## TCPDump

Tcpdump is a network capture and protocol analysis tool (www.tcpdump.org). This program is based on the libpcap interface, a portable system-independent interface for user-level network datagram capture. Despite the name, tcpdump can also capture non-TCP traffic, including UDP and ICMP. One of this tool's primary benefits is its wide availability, making it the de facto standard format for captured network traffic.

**Install TCP dump:**

sudo apt install tcpdump

**Check the interfaces:**

ip link show

**Capture the packets in a particular interface:**

sudo tcpdump -i *interface_name*

Explore all other options in TCPdump

## Socket Programming

Socket programming is a way of connecting two nodes on a network to communicate with each other. One socket(node) listens on a particular port at an IP, while the other socket reaches out to the other to form a connection. The server forms the listener socket while the client contacts the server.

https://www.youtube.com/watch?v=LtXEMwSG5-8
https://www.youtube.com/watch?v=mStnzIEprH8

## References


1. **https://www.tcpdump.org/manpages/tcpdump.1.html**
2. **https://www.cs.rpi.edu/~moorthy/Courses/os98/Pgms/socket.html**
3. **https://www.educative.io/answers/how-to-implement-tcp-sockets-in-c**